Application No.: 09/711,054   Docket No.: 102689-0065

REMARKS

Claims 1-33 are presently pending in the application. Applicants amend claims 1, 6, 12, 27 and 28, and add new claims 30, 31, 32, and 33 as listed above. The application is believed to be in condition for allowance. Hence, reconsideration and allowance are respectfully requested.

Rejections Under 35 U.S.C. § 112

The Office Action rejects claim 27 under 35 U.S.C. § 112, second paragraph, for twice reciting the limitation "retrieving a current set of identifiers". Claim 27 has been amended to state this limitation only once, thereby overcoming the rejection.

Rejections Under 35 U.S.C. § 102

The Office Action rejects claims 1-6, 12-21, 25, 26, and 28 as being anticipated by U.S. Patent No. 5,790,548 of Sistanizadeh et al.

Independent claim 1, as amended, recites a method of managing a telecommunications network that includes the steps of retrieving, through a management system, a current set of identifiers from a network device *where the identifiers comprise at least one physical identifier and one logical identifier*, and authenticating the identity of the network device using this set of identifiers. Support for amendments to claim 1 can be found, for example, on pages 5 and 244, in the original claims, and throughout the remainder of the specification. Thus, no new matter is added.

Sistanizadeh is directed to a method for providing internet access to one or more subscriber computers. When a subscriber computer comes online, the computer broadcasts a DHCP request to a DHCP server, which authenticates the computer based on the computer's media access control (MAC) address (col. 9, lines 63-67), and assigns a temporary IP address to that computer.

Sistanizadeh does not teach or suggest employing both a logical identifier and a physical identifier for authenticating a network device. Rather, in Sistanizadeh, a *single* physical identifier, namely a MAC address, is utilized for authenticating a subscriber's computer.

7

Application No.: 09/711,054   Docket No.: 102689-0065

Using both a physical identifier and logical identifier provides distinct advantages, such as enhanced fault tolerance and the ability to support hardware modularity (*See, e.g.,* specification, page 247, lines 15-26). For example, the use of a single physical identifier (such as the MAC address) associated with a board in a telecommunications device for authenticating that device can lead to a failure of authentication if that board is removed or replaced. In contrast, employing the board's physical identifier in conjunction with a logical identifier (e.g., the device's IP address) can allow authentication of the device even if the board is removed so long as the logical identifier has remained unchanged. Likewise, if the IP address changes, the network device can still be authenticated using a physical identifier, such as the MAC address. In other words, the multiple identifiers can provide a degree of redundancy that allow authenticating a device in case one (or possibly more) identifiers have been deleted or modified.

Thus, claim 1 distinguishes patentably over the Sistanizadeh reference. Claims 2-5, 13-21, 25, and 26, which depend either directly or indirectly on claim 1, not only incorporate the patentable features of claim 1 but also include additional features. For example, dependent claim 5 further recites that the logical identifier can be the device's IP address. Sistanizadeh does not teach employing an IP address of a device, together with a physical address, to provide a set of identifiers, each of which can provide authentication of that device. In fact, in Sistanizadeh, the DHCP server assigns an IP address to a computer *after* authenticating it based on a MAC address.

Claim 6, which is rewritten in independent format to include the features of the original claim 1, recites a method of managing a telecommunications network by detecting a request to add a network device to the telecommunications network, and retrieving an initial set of identifiers from the network device. The initial set of identifiers is stored in a storage unit that is accessible by a management system. The method further includes retrieving, through the management system, a current set of *at least two* identifiers from the network device, and authenticating the identity of the network device by comparing the retrieved current identifiers with the stored initial set, and authenticating the device if at least one of the current identifiers matches one of the stored initial identifiers.

8

As discussed above, Sistanizadeh does not authenticate a computer by matching one or more of *current* identifiers with their respective initially stored values. Hence, Sistanizadeh fails to teach salient features of claim 6.

Claim 12, which is rewritten in independent format to include the features of original claim 1, recites a method of managing a telecommunications network that comprises detecting a request to add a network device to the telecommunications network, retrieving an initial set of identifiers from the network device, converting the initial set of identifiers into a first composite value, and storing the first composite value in a storage unit accessible by a management system. The method further calls for retrieving, through the management system, a current set of identifiers from a network device, and authenticating the identity of the network device by employing the current set of identifiers. The authentication step includes dividing, for each retrieved identifier, the first composite value by one of the retrieved identifiers to form a division result, converting the remaining retrieved identifiers into a second composite value, and comparing the division result to the second composite value. The identity of the network device is authenticated if at least one of the division results matches one of the second composite values.

Sistanizadeh does not teach converting an initial set of identifiers retrieved from a network device into a composite value. Nor does it teach the other steps recited in claim 12 for authenticating the device based on a comparison of a current set of identifiers, and composite values generated from the current identifiers, with the composite value generated from the initial identifiers.

Accordingly, claim 12 distinguishes patentably over Sistanizadeh.

Sistanizadeh fails to teach or even suggest converting an initial set of identifiers into a composite value, and for each retrieved current identifier, dividing the composite value by one of the retrieved identifiers to form a division result.

9

Claim 28, as amended, recites a method of managing a telecommunications network comprising connecting a management system to a network device using a network address assigned to the network device, receiving a current set of *at least two* identifiers from a network device, and authenticating an identity of the network device using the current set of at least two identifiers.

The arguments presented above apply with equal force to establish that claim 28 is also patentable over Sistanizadeh.

Rejections under 35 U.S.C.§ 103

The Office Action rejects claims 7 and 29 as being obvious over Sistanizadeh.

Claim 7, which depends on claim 6, recites, among other elements, updating the stored identifiers with any of the retrieved current identifiers that do not match the stored initial identifiers.

Sistanizadeh does not teach authenticating a computer based on a subset of a plurality of retrieved identifiers that match corresponding identifiers in an initial set, and updating the remaining identifiers. As noted above, Sistanizadeh does not employ a plurality of identifiers, much less utilizing a subset of the identifiers for authentication while updating those that do not correspond to stored values. In fact, in Sistanizadeh, if the computer requesting an IP address does not have a correct MAC address, it cannot be authenticated.

Independent claim 29 is directed to a method of managing a telecommunications network comprising authenticating an identity of a network device using a current set of identifiers retrieved from the network device and a stored set of identifiers associated with the network device, and updating the stored set of identifiers when at least one but not all of the current identifiers match the stored identifiers.

As noted above, Sistanizadeh does not teach updating a stored set of identifiers when at least one current identifier matches a corresponding stored identifier. Hence, Sistanizadeh does not teach the advantages of the claimed method. In particular, in the method of claim 29, if at least one identifier matches a corresponding stored identifier, all the others can be updated. This

10

Application No.: 09/711,054   Docket No.: 102689-0065

allows changes to be made to the network device without authentication failure as long as at least one identifier remains unchanged. For example, a card in a network device can be removed and replaced with a new card without causing authentication failure so long as another identifier, e.g., a physical address of another card, remains unchanged. In addition, upon authentication, the stored value of the changed identifier is updated to reflect its current value, thereby maintaining current values for the stored identifiers. (see specification, page 248, lines 5-13).

The Office Action rejects claims 8 and 9 as being obvious over Sistanizadeh in view of "NetLinker FAQ".

Claims 8 and 9 depend, either directly or indirectly, on independent claim 6 and hence incorporate its features. The principal reference, Sistanizadeh, does not teach the use of more than one identifier for device authentication. And the secondary reference, "NetLinker FAQ" does not overcome the shortcomings of the principal reference. In particular, the "NetLinker FAQ" reference states that a message indicating failure means that a user-supplied name or password may be incorrect. It does not address authenticating a device based on a combination of physical and logical identifiers.

The Office Action rejects claims 10 and 11 are being unpatentable over Sistanizadeh in view of "NetLinker FAQ" and in further view of "TCP/IP Networking Concepts".

Claims 10 and 11 both depend, either directly or indirectly, on independent claim 6 and hence contain its features. Neither of the secondary references overcome the shortcomings of Sistanizadeh.

Claim 10 further recites detecting a user supplied new network address for the device, and updating a record associated with the network device with the new address. As an additional matter, the principal reference does not teach the features of claim 6, and hence those of claim 10, such as utilizing multiple current identifiers. Further, in Sistanizadeh, the IP address of a new network device is not user-supplied, but rather is assigned by the DHCP server. Moreover, the "NetLinker FAQ" reference is directed to messages concerning incorrect log-in names and passwords, and not to detecting a user-supplied *new* address for a network device, and updating a corresponding record containing that address. In addition, the Examiner's broad

11

Application No.: 09/711,054   Docket No.: 102689-0065

reference to TCP/IP concepts fails to provide any specific teaching that relates to the subject matter of claim 10.

The Office Action rejects claims 22-24 as being unpatentable over Sistanizadeh in view of U.S. Patent No. 6,059,446 of Ichimi, et al.

Claim 22-24 depend, either directly or indirectly, on independent claim 1, and thus contain all the limitations of claim 1. The principal reference, Sistanizadeh does not teach the use of at least one physical identifier and at least one logical identifier for device authentication, as recited in claim 1. The secondary reference, Ichimi, does not overcome this shortcoming of the principal reference. In particular, Ichimi is generally directed to LAN terminal equipment. It does not teach utilizing a current set of multiple identifiers for authenticating a device.

New Claims

New claim 30 recites a method of managing a telecommunications network comprising retrieving a current set of identifiers from a network device through a management system, where the identifiers comprise at least two physical identifiers, and authenticating the identity of the network device using the current set of identifiers. Claims 31-33 depend on claim 30 and add other features.

Support for these claims can be found, for example, on page 5 and throughout the remainder of the specification.

None of the cited references teaches the subject matter of claim 30, and the claims dependent on it. In particular, Sistanizadeh does not teach or suggest retrieving *at least two* physical identifiers from a device for authentication purposes.

12

Application No.: 09/711,054   Docket No.: 102689-0065
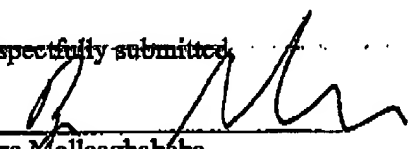
Conclusion

       In view of the above amendments and remarks, Applicants respectfully request reconsideration and allowance of the application. If there are any remaining issues, the Examiner if invited to call the undersigned at 617-439-2514.

Dated: November 17, 2004·   Respectfully submitted,

                                       By

                                       Reza Mollaaghababa
                                       Registration No.: 43,810
                                       NUTTER MCCLENNEN & FISH LLP
                                       World Trade Center West
                                       155 Seaport Boulevard
                                       Boston, Massachusetts 02210-2604
                                       (617) 439-2000
                                       (617) 310-9000 (Fax)
                                       Attorney for Applicant

1374572.1

13